Protection des données à caractère personnel

Louveaux, Sophie; de Terwangne , Cécile

Published in:
Actualités du droit des technologies de l'information et de la communication

Publication date:
2001

Document Version
le PDF de l'éditeur

PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL : APPLICATION EN BELGIQUE DE LA DIRECTIVE EUROPÉENNE

Sophie LOUVEAUX,
chercheur au CRID, (E consult)
et
Cécile de TERWANGNE,
assistante aux FUNDP

SOMMAIRE

Introduction

Nées en réponse aux préoccupations issues tout d'abord de l'apparition de l'informatique et ensuite des développements de l'ensemble des nouvelles technologies de l'information et de la communication, des législations de protection des données à caractère personnel ont peu à peu fleuri sur le territoire européen. La Convention du Conseil de l'Europe n° 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a consacré, au niveau européen, le droit de savoir de chacun à l'égard des données à caractère personnel le concernant. Les principes contenus dans la Convention 108 ont été précisés et amplifiés par la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données (1).

Une première loi fut votée en Belgique le 8 décembre 1992 (2), pour répondre à l'engagement contracté lors de la signature par le pays de la Convention 108. Une deuxième loi devait être adoptée pour le 24 octobre 1998 pour mettre la législation belge en conformité avec la directive européenne. Ce fut chose faite avec seulement quelques semaines de retard. La loi du 11 décembre 1998 (3) modifie assez radicalement la législation antérieure en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel.

(1) *J.O.C.E.*, n° L 281/31 du 23 novembre 1995. Voy. le considérant 11 de cette directive précisant explicitement la filiation existant entre la Convention 108 et la directive.
(2) Loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993.
(3) Loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 février 1999.

L'ensemble de ces législations visent explicitement à protéger les libertés et droits fondamentaux des personnes physiques, et notamment leur vie privée. La vie privée, dans ce contexte, est à entendre comme autodétermination informationnelle, c'est-à-dire comme autonomie dans la détermination des conditions de communication de données à caractère personnel (4). Ces législations participent à la consécration d'un droit de savoir des personnes. Ce droit de savoir est de portée individuelle. Il s'exerce par chacun à l'égard des données qui le concernent et qui sont conservées et utilisées par autrui. Il implique le droit pour les personnes « fichées » d'être informées du sort réservé aux données les concernant et le droit d'avoir accès à ces données.

Les pages qui suivent seront consacrées à l'analyse des conditions d'application des législations de protection des données à caractère personnel (section I), et aux deux principales conséquences découlant de l'application de ces législations aux traitements de données à caractère personnel : la question de la licéité des traitements (section II), et le respect du principe de transparence (section III).

(4) Voy. H. Burkert, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'Informatique et des Télécoms*, 1985, 8-16 ; C. de Terwangne, « Le rapport de la vie privée à l'information », in *Droit des technologies de l'information. Regards prospectifs* (sous la direction d'E. Montero), Cahier du CRID n° 16, Bruxelles, Bruylant, 1999, p. 144 ; Th. Leonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, *La vie privée : une liberté parmi les autres ?*, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.

Section I

Champ d'application de la législation relative à la protection des données à caractère personnel

A. La notion de « donnée à caractère personnel »

La loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel donne de la « donnée à caractère personnel » une définition textuellement reprise de la directive européenne en la matière (5). Par cette expression on entend « *toute information concernant une personne physique identifiée ou identifiable* », sachant qu'est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale (6) (7).

Dès lors qu'elles portent sur des individus identifiés ou identifiables, toutes informations sont qualifiées de « données à caractère personnel » au sens de la législation relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Il peut s'agir d'un numéro de plaque de voiture, de données contenues dans un ré-

(5) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 23 novembre 1995, n° L 281, p. 31.

(6) Art. 1er, § 1er nouveau de la loi belge du 8 décembre 1992.

(7) Pour savoir si l'évaluation du caractère identifiable doit se faire *in concreto*, en tenant compte des moyens à disposition du responsable du traitement des données, ou *in abstracto*, au regard des possibilités techniques existant pour d'autres, voy. M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux, D. Moreau, Y. Poullet, « La protection des données à caractère personnel en droit communautaire, *J.T. dr. eur.*, 1997, pp. 121 et s. Pour une comparaison entre le considérant 26 de la directive qui opte pour une évaluation *in abstracto* du caractère identifiable, et l'exposé des motifs de la nouvelle loi belge : Th. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, pp. 377 et s.

pertoire d'adresses, professionnel ou non, de photos, de données invisibles transmises lors de sessions Internet (adresses IP permanentes), de données bibliographiques, de l'identification des parties, des juges et des plaideurs dans les décisions de jurisprudence, etc.

Des statistiques pourtant anonymes peuvent, si elles présentent un niveau trop fin d'agrégation, soulever des difficultés au regard des principes issus de la législation de protection des données à caractère personnel. En effet, le caractère anonyme des informations statistiques peut être mis à mal par les techniques (pratiquées par les entreprises de marketing) consistant à identifier un petit groupe de population (correspondant à un îlot, niveau d'agrégation le plus fin) présentant des caractéristiques communes. Par des recoupements avec divers fichiers (données du recensement de la population, de l'annuaire téléphonique et du cadastre, par exemple), on parvient à l'identification des individus avec un très haut taux de probabilité. Des seuils minimaux d'agrégation sont donc à fixer pour que la diffusion de données statistiques anonymes ne heurte pas les droits garantis par la législation de protection des données (8).

B. Le traitement des données à caractère personnel

Pour que s'applique la législation de protection des données à caractère personnel, il faut être en présence d'un traitement de telles données. Les règles protectrices s'appliquent en effet à toute opération ou ensemble d'opérations effectuées en tout ou en partie à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel (9).

(8) Voy. l'avis de la Commission (française) Nationale de l'Informatique et des Libertés, *10e Rapport d'activité*, Paris, La Documentation française, 1989, pp. 11 et s.

(9) Art. 1er, § 2 et art. 3, § 1er nouveaux de la loi du 8 décembre 1992.

La loi s'applique également si ces opérations se font sans le moindre recours à des procédés automatisés, pourvu que les données sur lesquelles portent la ou les opérations soient contenues ou appelées à figurer dans un fichier (10). Par fichier, il faut entendre un « *ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* » (11). La notion de fichier se distingue de celle de « dossier ». La loi exclut les dossiers non structurés de son champ. Le critère de distinction entre fichier et dossier se situe dans le degré d'accessibilité des données contenues. Ces données doivent être accessibles selon des critères déterminés pour que l'ensemble soit considéré comme fichier (par exemple un classement sur la base des noms des personnes, par ordre alphabétique) (12).

Le champ d'application matériel de la loi est élargi par rapport au régime antérieur. Les opérations couvertes sont particulièrement variées et vont, cette fois, de la collecte à la consultation d'informations à caractère personnel, jusqu'à la communication par transmission, diffusion ou toute autre forme de mise à disposition de ces informations. Ces opérations correspondent en tout cas à un traitement de données si elles impliquent, ne fût-ce qu'en partie, le recours à des moyens automatisés. Il suffit, par exemple, que les informations soient au départ conservées sur un support informatisé et ensuite imprimées, ou qu'elles soient transmises en faisant usage de procédés automatisés, même si elles sont sur support papier (fax). Les moyens automatisés englobent toutes les technologies de l'information : informatique, télématique, réseaux de télécommunication.

(10) Art. 3, § 1er nouveau de la loi du 8 décembre 1992.

(11) Art. 1er, § 3 nouveau de la loi du 8 décembre 1992.

(12) La différence entre fichier et dossier a déjà fait couler beaucoup d'encre et a fait l'objet en Belgique d'un arrêt en cassation : Cass., 16 mai 1997, *J.T.*, 1997, p. 779 ; Anvers, 27 septembre 1995, *A.J.T.*, 1995-96, note J. Dumortier ; Th. Léonard, « La protection des données à caractère personnel et l'entreprise », in *Guide juridique de l'entreprise*, 2ème éd., Titre XI, Livre 112, Diegem, Kluwer, 1996, p. 15, n° 130 ; en France, voy. notamment : Cass. (ch. crim.), 3 novembre 1987, *D.*, 1988, J, pp. 17 et s., note H. Maisl ; T.G.I. Créteil, 10 juillet 1987, *D.*, 1988, J., pp. 319 et s., note J. Frayssinet ; J. Frayssinet, « La Cour de Cassation et la loi informatique, fichiers et libertés ou comment amputer une loi tout en raffermissant son application », *J.C.P.*, 1988, I, n° 3223 ; Idem, « Contre l'excessive distinction entre fichier et dossier – La pas en avant du tribunal correctionnel de Paris », *Expertises*, 1990, pp. 16 et s.

Lorsqu'aucun procédé automatisé n'intervient dans les opérations effectuées sur les informations, la législation de protection des données à caractère personnel ne s'appliquera pas si les informations proviennent de dossiers, ou de documents non classés dans un fichier. La consultation de documents papier isolés ou l'envoi par courrier ordinaire de photocopies de documents papier qui ne sont pas extraits d'un « *ensemble structuré de données à caractère personnel accessibles selon des critères déterminés* », peuvent se faire, par exemple, sans tenir compte des principes régissant la protection des données à caractère personnel.

Il est à noter que les dispositions contenues dans la législation de protection des données à caractère personnel s'appliquent tant au secteur public qu'au secteur privé. Il est donc indifférent, pour la prise en compte des principes de protection des données, que le détenteur des informations soit une entité publique ou privée.

C. Le responsable du traitement

La notion de « responsable du traitement » désigne la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (14). Dans l'exposé des motifs du projet de la future loi relative à la protection des données à caractère personnel du 11 décembre 1998, adaptant la loi

(14) Art. 1er , § 4 nouveau de la loi du 8 décembre 1992. Sur la préférence à accorder au seul critère du pouvoir de détermination des finalités, voy. M.-H. Boulanger, C. de Terwangne, Th. Léonard, « La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personne », *J.T.*, 1993, p. 373, n° 16.

belge de 1992 à la directive européenne en la matière, le ministre a précisé que c'est la personne investie du pouvoir de décision sur le traitement de données qui est visée par la notion de responsable du traitement (15).

Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable du traitement est la personne physique ou morale, l'association de fait ou l'administration publique désignée comme tel par le texte en question (16).

D. Les exceptions

Des exceptions sont prévues, soit globales, soustrayant certains traitements de données à l'ensemble de la loi, soit partielles, dispensant du respect de certaines dispositions de la loi. Bénéficient de l'exception globale les traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques (17).

Les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire entrent, eux, dans la catégorie d'exceptions partielles. Une série de dispositions peuvent ne pas être appliquées à ces traitements, afin de garantir un équilibre avec la protection de la liberté d'expression (18).

D'autres exceptions partielles, pour classiques qu'elles soient, sont particulièrement larges. Il s'agit des exceptions accordées aux traitements effectués à des fins de sécurité publique (19). Il est étonnant et particulièrement dommage que ces exceptions n'aient fait l'objet d'aucun débat au sein de la société, ou à tout le moins au sein du Parlement, au moment de leur adoption. D'autant que « *la loi consacre un dangereux déséquilibre entre les impératifs légitimes de la sécurité de l'Etat*

(15) Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Exposé des motifs, *Doc. Parl.*, Ch. Repr., sess. ord. 1997-1998, n° 1566/1, p. 15.
(16) Art. 1er, § 4, al. 2 nouveau de la loi du 8 décembre 1992.
(17) Art. 3, § 2 nouveau de la loi du 8 décembre 1992.
(18) Art. 3, § 3 nouveau de la loi du 8 décembre 1992.
(19) Art. 3, §§ 4 et 5 nouveau de la loi du 8 décembre 1992.

et de sa défense et les intérêts de la personne concernée dans la mesure où la loi affaiblit de manière disproportionnée les possibilités de contrôle du respect des prérogatives liées à la protection des données » (20).

E. Le champ d'application territoriale de la loi

Le législateur belge, suivant la directive, a modifié le critère de rattachement déterminant l'applicabilité de la loi. Il s'est définitivement écarté de la notion de « fichier », déterminante dans les premières générations de législations en la matière et basée sur une localisation physique précise des données (sur une disquette, sur le disque dur d'un ordinateur identifié,...). Il n'a plus retenu non plus la localisation du traitement, celui-ci pouvant désormais être effectué sur des données qui ne sont pas rassemblées dans un « lieu » unique. C'est le lieu d'établissement fixe (21) du responsable du traitement qui est à présent le critère d'applicabilité de la loi (22). Si le responsable d'un traitement a un établissement fixe sur le territoire belge, c'est la loi belge qui s'appliquera au traitement effectué par le responsable dans le cadre des activités réelles et effectives de cet établissement. Ainsi, si un complexe hôtelier localisé en Belgique offre un service de réservation via Internet et demande en conséquence aux intéressés d'enregistrer leurs coordonnées afin d'effectuer la réservation, la loi belge de protection des données trouvera à s'appliquer au traitement de ces informations.

À l'instar du législateur européen, le législateur belge s'est préoccupé des tentatives de contournement du régime de protection mis en place, par la délocalisation de l'établissement du responsable du traitement. Afin d'éviter pareille situation, le texte (23) prévoit que tout responsable qui n'est pas établi de manière permanente sur le territoire de la Communauté européenne mais qui recourt à des moyens, automatisés

(20) Y. Poullet et B. Havelange, « Secrets d'Etat et vie privée ou comment concilier l'inconciliable ? », in *Droit des Technologies de l'information Regards prospectifs*, Cahier du CRID n° 16, Bruxelles, Bruylant, 1999, n° 15.

(21) Le considérant 19 de la directive 95/46/CE précise que "*l'établissement sur le territoire d'un Etat membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable. [...] La forme juridique retenue pour un tel établissement, qu'il s'agisse d'une simple succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à ce sujet*".

(22) Art. 3*bis*, al. 1er, 1° nouveau de la loi du 8 décembre 1992.

(23) Art. 3*bis*, al. 1er, 2° nouveau de la loi du 8 décembre 1992.

ou non, situés sur le territoire belge, dans le but de traiter des données personnelles, est soumis à la loi du 8 décembre 1992 modifiée. Il est tenu en outre de désigner un représentant établi sur le territoire belge (24). Le seul transit de données sur le territoire belge n'est toutefois pas couvert par la loi.

Dans le monde en réseau que nous connaissons, et principalement dans le contexte d'Internet, une telle solution est excessive et impraticable. Elle conduit en effet à étendre l'application de la loi belge à tout utilisateur d'Internet qui copie ou télécharge des informations nominatives à partir d'un site Web ouvert par un fournisseur d'informations établi en Belgique (25). Ce faisant, l'internaute effectue en effet un traitement de données en recourant à des moyens automatisés (26) situés en Belgique. Il est donc tenu de respecter la loi belge et de désigner un représentant établi dans notre pays. Il en va de même pour tout responsable de site Web de par le monde qui invite les internautes, via le site, à communiquer des informations nominatives. Lorsqu'un internaute communique ses données par des moyens situés sur le territoire belge (son ordinateur, les installations de son fournisseur d'accès, les appareils de télécommunications), la collecte réalisée par le responsable du site est désormais soumise à la loi belge et le responsable doit désigner un représentant en Belgique. C'est assurément irréaliste.

Pour garder à l'article 3*bis* une portée effective, la seule lecture de cette disposition qui, à notre sens, s'impose, est une lecture téléologique. La *ratio legis* de cet article se résume clairement dans la volonté d'éviter que les individus se retrouvent dépourvus de toute protection, en particulier du fait d'un contournement de la législation (27). Le souci des

(24) Art. 3*bis*, al. 2 nouveau de la loi du 8 décembre 1992.

(25) Sur le raisonnement attaché à cet exemple, voy. M.-H. Boulanger et C. de Terwangne, "Internet et le respect de la vie privée", in *Internet face au droit*, Cahier du CRID n° 12, Bruxelles, Story-Scientia, 1997, pp. 201-202.

(26) L'exposé des motifs de la loi du 11 décembre 1998 signale que "*le terme "moyens" recouvre tout équipement possible, tels que les ordinateurs, les appareils de télécommunications, les unités d'impression, etc., à l'exclusion, formulée explicitemement, des moyens qui sont uniquement utilisés pour le transit des données à caractère personnel par le territoire, tels que les câbles, les routes, etc.*" (*Doc. parl.*, Ch. repr., sess. ord. 1997-98, n° 1566/1, p. 27).

(27) Voy. l'exposé des motifs (*Doc. parl.*, Ch. repr., sess. ord. 1997-98, n° 1566/1, p. 27) et le considérant 20 de la directive.

auteurs du texte est donc d'assurer une protection à ceux qui doivent normalement en bénéficier sous l'égide de la loi, même en dehors des frontières.

C'est par une lecture combinée de l'article *3bis* et des articles 21 et 22 qui régissent les flux transfrontières vers les Etats non membres de la Communauté européenne qu'une définition rationnelle de l'applicabilité de la loi pourra être dégagée.

On peut en effet considérer qu'une première réponse à la préoccupation du législateur est donnée par l'instauration d'un régime protecteur en matière de flux transfrontiers de données en dehors de la Communauté européenne. Dans le cadre de la réglementation de ces flux, les exigences édictées par la loi s'imposent à tous les acteurs qui effectuent des opérations sur des données transférées à partir de la Belgique. Une protection adéquate des données envoyées à l'étranger en provenance de Belgique est exigée.

La réponse contenue à l'article *3bis* vise à couvrir, quant à elle, les situations dans lesquelles les sujets des données se voient privés, par une manœuvre artificielle, du bénéfice de la protection de l'ensemble de la loi, et les situations échappant à toute protection, même celle instaurée en matière de flux transfrontiers. Dans ce sens, deux catégories de situations entrent selon nous, dans le champ de l'article *3bis* :

- celle précisément où un responsable de traitement cherche délibérément à contourner la directive et, pour ce faire, délocalise son établissement vers un pays tiers, tout en faisant usage de moyens localisés sur le territoire belge pour réaliser son traitement ;
- celle où le flux est le fait exclusif d'un responsable localisé dans un pays tiers. C'est le cas d'une collecte de données effectuée par le biais de *cookies*, à l'insu de la personne concernée, au sein même de son ordinateur. Les *cookies* auront été discrètement déposés par le responsable d'un site Internet sur le disque dur du « surfeur » belge, à l'occasion d'une de ses visites du site en question. Les dispositions concernant les flux transfrontiers de données ne trouvent pas à s'appliquer à cette hypothèse (28). Pour combler le vide de protection, l'article *3bis* a alors toute sa pertinence. C'est donc le régime complet de la directive qui va s'appliquer au traitement de données obtenues à l'aide de *cookies*, et non le régime spécifique -plus souple- des flux transfrontiers.

(28) Voy. l'explication détaillée donnée dans M.-H. Boulanger et C. de Terwangne, *op. cit.*, p. 203.

Dans ces deux hypothèses, le critère déterminant de l'application de la loi belge aux responsables établis hors de la Communauté européenne ne se réduit pas à l'utilisation de moyens situés sur le territoire du pays. Cette utilisation n'est qu'un élément de l'analyse du contexte des opérations effectuées. Une analyse plus globale s'impose en effet pour pouvoir constater le cas échéant que le responsable du traitement est anormalement établi à l'étranger alors que son activité est orientée sur la Belgique, ou que l'on se trouve en présence d'une situation échappant à toute protection, notamment à celle issue du régime des flux transfrontiers.

Section II

Licéité des traitements de données à caractère personnel

La directive européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données prévoit les conditions auxquelles un traitement des données doit répondre pour être admissible (29). Ces conditions ont été reproduites dans la loi belge (30).

Avant de passer en revue ces conditions, il y a lieu de préciser qu'un régime particulier est réservé aux données dites « sensibles ». Une série de données à caractère personnel ont été qualifiées de « sensibles » par la Convention n° 108 du Conseil de l'Europe (31) car elles sont susceptibles, par leur nature, de porter atteinte aux libertés fondamentales et notamment à la vie privée des personnes concernées. Reprise dans la directive communautaire (32) et dans les lois nationales, dont la loi belge (33), cette catégorie de données concerne les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la santé, la vie sexuelle et les données relatives aux infractions et condamnations pénales (34). L'arrêté royal destiné à préciser le régime particu-

(29) Art. 6 et 7 de la directive du 24 octobre 1995.
(30) Art. 4 et 5 nouveaux de la loi du 8 décembre 1992.
(31) Art. 6 de la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
(32) Art. 8 de la directive du 24 octobre 1995.
(33) Art. 6, 7 et 8 nouveaux de la loi du 8 décembre 1992.
(34) La directive admet potentiellement qu'entrent également dans cette catégorie les données relatives aux sanctions administratives ou aux jugements civils (art. 8, § 5, al. 2). La loi belge est particulièrement large concernant les « données judiciaires » : aux termes de son article 8, elle vise les données « *relatives à des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, à des suspicions, des poursuites ou des condamnations ayant trait à des infractions, ou à des sanctions administratives ou des mesures de sûreté* ».

lier des données sensibles n'est, à cette date (début janvier 2001), pas encore paru au Moniteur belge.

A. L'utilisation de données à caractère personnel comme traitement à part entière

1. Le respect du principe de finalité

Pour être licite, l'utilisation de données à caractère personnel doit répondre aux exigences appliquées à tout traitement à part entière. Elle doit poursuivre une finalité déterminée, explicite et légitime (35) et s'identifier à une des hypothèses reprises dans la liste de l'article 5 de la loi de 1992.

Déterminée et explicite, la finalité de la communication ne peut être secrète, camouflée.

La finalité de la communication doit en outre être légitime. Bien que ce terme ne soit pas explicitement précisé dans la législation de protection des données, la doctrine s'accorde pour estimer que pour être légitime, la finalité ne peut induire une atteinte disproportionnée aux intérêts de la personne concernée par les données, au nom des intérêts poursuivis par le responsable du traitement (36). La notion de légitimité invite donc à une mise en balance des intérêts en présence.

Par ailleurs, l'article 5 nouveau de la loi du 8 décembre 1992 (37) énonce les six seules hypothèses dans lesquelles un traitement de données peut être effectué. Ces hypothèses représentent en fait les situations dans lesquelles l'équilibre des intérêts en présence est *a priori* atteint. M.-H. Boulanger, intervenant au nom de la Commission (belge) de la protection de la vie privée, signala lors des discussions qui accompagnèrent le

(35) Art. 4, § 1e, 2° de la loi du 8 décembre 1992.

(36) M.-H. Boulanger, C. de Terwangne, Th. Léonard, *op. cit.*, pp. 377 et 379 ; Th. Léonard, Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur n° 17, Bruxelles, Larcier, 1992, pp. 231 et s. ; S. Gutwirth, « De toepassing van het finaliteitbeginsel van de privacywet van 8 december 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », *T.P.R.*, 1993/4, pp. 1409 et s. ; J. Dumortier, F. Robben, note sous Com. Anvers (Prés.), 7 juillet 1994 et Com. Bruxelles (Prés.), 15 septembre 1994, *Computerrecht*, 1994, pp. 244 et s.

(37) Reproduction de l'article 7 de la directive du 24 octobre 1995.

vote de la modification de la loi belge, que les situations visées par l'article 5 de la loi créent « une présomption d'équilibre d'intérêts » (38).

Les deux dispositions doivent être lues conjointement. Le fait de se trouver dans une des situations énoncées à l'article 5 n'implique pas que l'exigence de légitimité de l'article 4 soit *ipso facto* rencontrée. Les hypothèses visées dans la deuxième disposition n'empêchent pas un contrôle sur la base de la première. En fait, on peut considérer que l'article 5 prévoit des situations abstraites dans lesquelles l'équilibre des intérêts en présence est normalement respecté, sans préjudice d'un contrôle concret, sur la base de l'article 4, permettant, le cas échéant, de révéler une atteinte inacceptable aux droits et intérêts de l'individu (39).

Au titre des hypothèses autorisant le traitement de données, on trouve le consentement indubitable de la personne concernée (40), le cas du traitement « *nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci* » (41), du traitement « *nécessaire au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance* » (42), du traitement « *nécessaire à la sauvegarde de l'intérêt vital de la personne concernée* » (43), du traitement « *nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées* » (44) et enfin, du traitement « *nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée* » (45).

(38) In Rapport fait au nom de la Commission de la justice, *Doc. parl.*, ch. repr., sess. ord. 1998-1999, n° 1566/10, p. 47.

(39) M.-H. Boulanger, C. de Terwangne, Th. Leonard, S. Louveaux, D. Moreau, Y. Poullet, *op. cit.*, p. 148, n° 41.

(40) Art. 5, al. 1er, *littera* a de la loi du 8 décembre 1992.

(41) Art. 5, al. 1er, *littera* b de la loi du 8 décembre 1992.

(42) Art. 5, al. 1er, *littera* c de la loi du 8 décembre 1992.

(43) Art. 5, al. 1er, *littera* d de la loi du 8 décembre 1992.

(44) Art. 5, al. 1er, *littera* e de la loi du 8 décembre 1992.

(45) Art. 5, al. 1er, *littera* f de la loi du 8 décembre 1992.

2. *L'impact des nouvelles potentialités techniques sur le caractère légitime de la finalité*

La publicité de données à caractère personnel peut dans certains cas découler d'obligations fixées par la législation. C'est le cas, par exemple, de la mise à disposition du public de guides présentant le personnel des administrations, conformément à l'obligation contenue dans la législation relative à la transparence de l'administration. La licéité de l'opération de transmission des données à caractère personnel tient au fait, dans ces cas, que de tels traitements entrent dans la catégorie des traitements nécessaires au respect d'une obligation légale.

Il faut toutefois s'assurer que les conditions de mise à disposition de l'information garantissent le respect de cette finalité légitime. L'accessibilité d'informations à caractère personnel par la voie numérique suscite le risque particulier que l'accès aux informations ne se fasse pas dans le souci auquel le législateur a voulu répondre par l'obligation de publicité, mais dans une perspective détournée. Les possibilités de recherche dans une masse de documents sur la base de critères variés, les possibilités d'obtenir l'ensemble des données contenues dans un registre, sous une forme facilement réutilisable, peuvent conduire à des détournements de finalité de la publicité des données.

Ainsi, diffusé sur support informatisé (CD-ROM ou diffusion sur Internet), l'annuaire téléphonique pourrait être téléchargé en entier pour permettre une réutilisation commerciale des informations (mailings, croisement avec d'autres fichiers). On s'éloigne radicalement du souci de connaître le numéro d'appel d'un abonné afin d'établir une communication téléphonique. L'équilibre atteint en regard de la finalité initiale de diffusion des informations est rompu. L'atteinte au droit des personnes concernées est disproportionnée par rapport à l'intérêt des tiers en jeu.

De même, la constitution et la mise à disposition d'une base de données jurisprudentielles permet de recueillir « *l'ensemble de la jurisprudence relative à des licenciements pour motifs graves, pour en extraire les noms et adresses des employés mis en cause* » ou d'identifier « *aisément les médecins dont la responsabilité aura été poursuivie devant les tribunaux. Le comportement d'un juge face à tel ou tel type de conflits pourra être évalué statistiquement et le nom d'un*

avocat pourra être associé à un pourcentage d'issues favorables d'un procès » (46). Par ailleurs, interroger une base de données jurisprudentielles par le critère du nom des parties permet de retrouver, pour un individu, toutes les condamnations dont il a fait l'objet. Cette possibilité technique de reconstituer l'histoire judiciaire d'une personne « *engendre des risques en matière de protection des données sans commune mesure avec ceux liés aux modes traditionnels d'accès ou de publication de la jurisprudence* » (47).

La Commission belge de la protection de la vie privée a marqué sa préoccupation pour la question. Dans son avis du 22 avril 1996, elle note : « *Les recherches automatisées habituelles dans du texte libre, disponibles dans les logiciels de consultation des CD-ROM ou des réseaux comme Internet, permettent, en effet, d'opérer des sélections dans de vastes recueils de prononcés sur la base des noms des parties, en combinaison avec d'autres critères de recherche, dont on peut déduire de façon systématique des informations concernant la vie privée des personnes identifiées. Selon la Commission, l'apparition de pareilles difficultés en raison de l'évolution technologique doit s'accompagner d'une plus grande retenue lors de la mention de ces données pouvant mener à l'identification des parties dans les chroniques automatisées de jurisprudence et lors de la recherche d'autres systèmes visant à identifier des prononcés judiciaires* » (48).

Les nouveaux risques liés au développement des technologies de l'information et de la communication se résument en une accessibilité des informations indépendante du lieu, des frontières et du temps ; une conservation longue durée (« the eternity effect » (49)) : la mémoire électronique ne permet plus le droit à l'oubli ; des utilisations secondaires incontrôlées des informations ; le profilage des individus.

(46) Y. Poullet, « Autour de l'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'Etat : les technologies de l'information et de la communication, une solution à la pathologie législative ? », in *La pathologie législative, comment en sortir ?*, coll. Droit en Mouvement, Bruxelles, La Charte, 1998, p. 70.

(47) *Ibid.*, p. 71. Voy. également S. Walz, *" Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society ", contribution présentée à la 19ème Conférence internationale des Commissaires à la protection des données, Bruxelles, 17-19 septembre 1997.* p. 3 : « */.../ reports about convictions long after the sentence has been served are published in multimedial forms, usable for surveillance, credit information or other purposes related to civil life and accessible worlduide* ».

(48) Avis n° 07/96.

(49) S. Walz, *op. cit.*, p. 3.

Créant de nouveaux dangers pour la vie privée des individus, les nouvelles technologies de la communication et de l'information modifient l'équilibre atteint dans un contexte traditionnel. Les conditions d'un nouvel équilibre entre les intérêts contradictoires en présence doivent en conséquence faire l'objet d'une nouvelle évaluation (50).

B. L'utilisation des données à caractère personnel comme traitement compatible avec la finalité de collecte des données

Aux termes de l'article 4, § 1er, 2° de la loi belge de protection des données, les données à caractère personnel doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [...]* » (51).

1. Compatibilité ou incompatibilité

Dans certaines hypothèses, l'utilisation des informations à caractère personnel pourra être considérée comme compatible avec les finalités pour lesquelles ces informations ont été recueillies.

La loi belge précise que pour évaluer la compatibilité des utilisations des données survenant ultérieurement à la collecte, il faut tenir compte de tous les facteurs pertinents, et notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. En ce sens, on peut considérer que le critère de compatibilité est

(50) Dans le même sens, H. BURKERT, « The Commercial Use of Government Controlled Information and its Information Law Environment in the EEC », " The Commercial Use of Government Controlled Information and its Information Law Environment in the EEC ", in W.F. KORTHALS ALTES, E.J. DOMMERING, P.B. HUGENHOLTZ, J.J.C. KABEL (ed.), *Information Law towards the 21st Century*, Deventer, Boston, Kluwer Law and Taxation Publishers, 1992. p. 232 : « *there was a large body of register laws which provided for the collection of personal information in order to make such information public. Very often, these laws gave a general unrestricted right of access to personal information. [...] Register legislation, however, has been coined for traditional – paper file – registers. These registers had a number of 'built-in' restrictions which had served as tacit protection mechanisms. Where such registers turn automatic they usually provide a new quality of accessibility which has to be reconsidered. This reconsideration again has to take into account the reasons for which these traditional registers had provided general access (e.g. to guarantee the integrity of the voting process or of business corporations)* ».

(51) Cette disposition est une reprise littérale de l'art. 6, § 1er, *littera* b, première phrase, de la directive du 24 octobre 1995.

lié à l'un des principes majeurs de la législation de protection des données, à savoir la transparence des traitements de données à l'égard des personnes concernées par les données. Ce principe implique que la personne sur qui portent les données connaisse en toutes circonstances les utilisations qui sont faites des données. Le critère de compatibilité des traitements ultérieurs est donc logique lorsqu'il renvoie à la connaissance effective ou à l'attente raisonnable de la personne concernée (52) (53).

Dans de nombreux autres cas, l'utilisation de données à caractère personnel ne pourra passer pour compatible avec les finalités poursuivies lors de la collecte de ces informations.

Une communication à des fins commerciales (54) des données à caractère personnel recueillies par l'administration ne pourra, par exemple, au vu des considérations émises sur le critère de compatibilité, être considérée comme compatible avec les finalités de collecte. On ne peut, en effet, faire entrer dans l'attente raisonnable des personnes communiquant des données à une personne publique dans le cadre d'un rap-

(52) C'est ce critère qui avait été suggéré *in* C. DE TERWANGNE et S. LOUVEAUX, « Data Protection and Online Networks », *Computer Law and Security Report*, 1997, vol. 13, n° 4, p. 239 et *in* M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, *op. cit.*, p. 146, n° 32.

(53) Le recours aux dispositions légales et réglementaires pour évaluer la compatibilité d'utilisations ultérieures ne devrait pas renier ce lien avec le principe de transparence à l'égard de la personne concernée puisque l'Exposé des motifs de la loi spécifie que « *la mesure dans laquelle et la manière dont les personnes concernées ont préalablement été informées du nouveau traitement par les autorités jouera un rôle important lors de l'évaluation de la compatibilité ou de l'incompatibilité du traitement avec la finalité initiale pour laquelle les données ont été obtenues* » (Projet de loi transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 1997-1998, n° 1566/1). Le système belge n'opte pas, semble-t-il, pour une compatibilité automatique découlant de la seule existence de dispositions légales ou réglementaires. C'est particulièrement souhaitable étant donné que l'obligation d'information des personnes concernées, existant par ailleurs et pesant normalement sur tout responsable d'un traitement de données, n'existe pas pour les traitements prévus par la loi. Voy. également J. DUMORTIER, « Some legal issues related to the implementation of the European data protection Directive in the Belgian legal system », contribution présentée à la 19ème Conférence internationale des Commissaires à la Protection des Données, Bruxelles, 17-19 septembre 1997, p. 6.

(54) Les finalités commerciales sont envisagées ici tant dans le chef du secteur public : c'est l'administration qui souhaite vendre ses données, que dans le chef d'un tiers privé : c'est l'entreprise qui acquiert les données pour les intégrer dans un produit informationnel qu'elle veut commercialiser.

port réglé par la loi (communication légalement obligatoire ou effectuée pour bénéficier d'un service public), une réutilisation commerciale de ces données.

2. Conséquences pratiques de la distinction

Les conséquences du caractère compatible ou non de l'utilisation avec les finalités initiales de collecte des informations ne sont pas négligeables.

Si elle est considérée comme compatible avec les finalités initiales, l'utilisation ne devra pas elle-même passer le test de la légitimité imposé par l'article 4, § 1er, 2°. Ce sont les finalités initiales qui auront dû être jugées légitimes. Toute utilisation compatible avec ces finalités légitimes est admissible en soi. En outre, compatible avec les finalités de collecte, l'utilisation ne constitue pas un traitement indépendant. Elle ne doit dès lors pas non plus répondre à l'une des hypothèses de licéité des traitements contenue dans l'article 5 nouveau de la loi du 8 décembre 1992. Chaque traitement en soi (indépendant) doit correspondre à une de ces hypothèses de licéité, tandis que les « utilisations compatibles » ne sont pas concernées comme telles par cette exigence.

Par contre, les utilisations qui ne sont pas compatibles avec les finalités de collecte ne peuvent être rattachées au traitement initial des données. Elles doivent être envisagées comme des traitements séparés, indépendants, et doivent dès lors répondre elles-mêmes à toutes les exigences édictées par la loi pour admettre un traitement comme licite.

Section III
Le principe de transparence

A. Devoir d'information pesant sur les détenteurs de données à caractère personnel

1. Principe

Tout responsable de traitement de données à caractère personnel est tenu de fournir certaines informations aux personnes concernées par les données. Cette formalité doit être accomplie soit au moment de l'obtention des données, lorsque les données sont obtenues de la personne concernée elle-même, soit au plus tard au moment de la première communication des données, lorsque les données ont été obtenues de manière indirecte (55).

Les informations à fournir consistent en :

- les coordonnées du responsable du traitement (nom et adresse),
- les finalités du traitement,
- l'existence du droit de s'opposer gratuitement au traitement envisagé à des fins de *direct marketing*,
- les destinataires ou catégories de destinataires des données,
- l'existence d'un droit d'accès et de rectification des données,
- le caractère obligatoire ou non des réponses ainsi que les conséquences d'un défaut éventuel de réponse (lorsque les données sont collectées auprès de la personne concernée) et
- les catégories de données (lorsque les données sont obtenues de source indirecte).

(55) Art. 10 et 11 de la directive du 24 octobre 1995 et art. 9 nouveau de la loi du 8 décembre 1992.

Les quatre derniers types d'information à fournir ne doivent pas être communiqués si, compte tenu des circonstances particulières dans lesquelles le traitement est effectué, cela n'est pas nécessaire pour assurer un traitement loyal des données (56).

Lorsque les données n'ont pas été recueillies directement auprès des personnes concernées et qu'une utilisation à des fins de *direct marketing* est envisagée, le responsable a l'obligation d'informer les personnes concernées avant que les données ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers. Cela doit permettre aux personnes concernées d'exercer utilement le droit d'opposition qui leur est reconnu.

2. Exceptions

Le responsable du traitement est dispensé d'informer la personne concernée si celle-ci a déjà connaissance des informations à fournir (57). L'exception n'est valable qu'en présence de personnes déjà « informées » et non « raisonnablement supposées informées ».

Dans les cas où les données ont été obtenues de source indirecte, les responsables de traitement de données sont en outre dispensés de fournir l'information dans deux hypothèses :

- lorsque l'information des personnes concernées se révèle impossible ou implique des efforts disproportionnés ; cette hypothèse peut apparaître notamment dans le cas de traitements à des fins statistiques ou de recherche historique ou scientifique, ou pour le dépistage motivé par la protection et la promotion de la santé publique (58) ;

(56) Il est à noter que la directive prévoit, de manière inversée, que les informations supplémentaires à fournir (les quatre dernières catégories d'informations) ne doivent être communiquées par le responsable que si elles sont nécessaires pour assurer un traitement loyal des données. Sur la nécessité des informations au vu du traitement loyal des données, voy. C. DE TERWANGNE et S. LOUVEAUX, « Data Protection and On Line Networks », *Computer Law & Security Report*, 1997, vol. 13, n° 4 ; M.-H. BOULANGER, C. DE TERWANGNE, TH. LEONARD, S. LOUVEAUX, D. MOREAU, Y. POULLET, *op. cit.*, p. 150, n° 53.

(57) Art. 9, § 1er et § 2, al. 1er nouveau de la loi du 8 décembre 1992.

(58) Art. 9, § 2, al. 2, *littera* a nouveau de la loi du 8 décembre 1992.

- si l'enregistrement ou la communication des données est effectuée en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance (59).

Pour cette dernière hypothèse, la directive a en fait énoncé de façon bien plus stricte l'exception au devoir d'information. La version belge permet au pouvoir exécutif de lever l'obligation d'information, au nom sans doute d'une quelconque efficacité, sans que cela fasse l'objet d'un débat dans une assemblée parlementaire. La directive n'admet, elle, de dispenser le responsable du traitement de fournir les informations requises aux personnes concernées que « *si la législation prévoit expressément l'enregistrement ou la communication des données* » (60). Il faut donc que l'enregistrement ou la communication des données soit clairement prévu par la législation.

B. Droit d'accès

1. Accès direct

Les personnes qui procèdent au traitement de données à caractère personnel sont tenues de communiquer aux personnes concernées qui le demandent la confirmation du traitement ou non de données à leur sujet, ainsi que les finalités du traitement, les catégories de données traitées et les catégories de destinataires des données (61).

Les responsables du traitement doivent aussi communiquer sous une forme intelligible les données faisant l'objet du traitement ainsi que toute information disponible sur l'origine des données (62). Inexistante en Belgique avant l'adaptation à la directive européenne, cette obligation d'information sur l'origine des données, qui sera logiquement d'application lorsque les données n'auront pas été recueillies directement auprès de la personne concernée, est d'un intérêt certain étant donné que c'est souvent la question de la source des informations qui préoccupe les personnes concernées.

(59) Art. 9, § 2, al. 2, *littera* b de la loi du 8 décembre 1992.

(60) Art. 11, § 2 de la directive du 24 octobre 1995.

(61) Art. 10, § 1er, al. 1er, *littera* a nouveau de la loi du 8 décembre 1992.

(62) Art. 10, § 1er, al. 1er, *littera* b nouveau de la loi du 8 décembre 1992.

Lorsqu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative est prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, cette personne doit pouvoir obtenir du responsable du traitement la connaissance de la logique qui sous-tend le traitement automatisé en question (63).

Pour exercer son droit d'accès, la personne concernée doit adresser une demande écrite au responsable du traitement. Celui-ci doit répondre sans délai et au plus tard dans les quarante-cinq jours de la réception de la demande.

Le droit d'accès offre à la personne concernée une autre voie pour obtenir des informations sur les traitements effectués sur ses données. Cette voie n'offre toutefois pas les mêmes garanties que le devoir d'information pesant sur le responsable du traitement car elle exige une démarche de la part de la personne concernée, celle-ci devant au demeurant avoir déjà connaissance de l'identité du responsable du traitement. Le droit d'accès ne compense donc pas, en termes d'information de la personne concernée sur le sort réservé à ses données, la formulation trop large de l'exception au devoir d'information présente dans la loi belge remodelée.

2. Accès indirect

En deux circonstances, la loi a prévu une formule d'accès indirect de la personne concernée à ses données.

L'accès d'une personne aux données à caractère personnel relatives à sa santé peut ainsi s'effectuer soit directement, soit par l'intermédiaire d'un professionnel des soins de santé (64) choisi par elle, si le responsable du traitement, voire elle-même, demande l'intervention d'un intermédiaire (65). La loi n'impose aucune motivation particulière de la part du responsable du traitement pour justifier le refus d'accès direct et la

(63) Art. 10, § 1er, al. 1er, *littera* c nouveau de la loi du 8 décembre 1992.

(64) Par « professionnel des soins de santé », il conviendrait d'entendre un médecin et non d'autres professionnels tels les infirmières ou pharmaciens. Voy. Th. Leonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *op. cit.*, note 135.

(65) Art. 10, § 2 nouveau de la loi du 8 décembre 1992.

demande d'intervention d'un intermédiaire. La formule risque donc d'amener les responsables de traitements à exiger systématiquement l'accès indirect aux données médicales qu'ils contrôlent.

C'est également un accès indirect qui est mis en place pour les données faisant l'objet de traitements effectués à des fins de sûreté de l'Etat, de sécurité publique, de défense nationale, de prévention ou de répression des infractions (66). Dans ces cas, c'est par l'intermédiaire de la Commission de la protection de la vie privée que le droit d'accès peut s'exercer. Après avoir exercé ce droit, ladite Commission spécifie uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires. Cette formule d'un accès indirect systématique pour les données en question est critiquable. L'article 13 de la directive qui autorise une telle limitation au principe du droit d'accès direct ne le fait que s'il s'agit d'une mesure « *nécessaire pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique, la prévention et la poursuite d'infractions pénales [...]* ». Il n'est donc pas question de limitation automatique (67).

C. Droit de rectification

Toute personne concernée peut, sans frais, faire rectifier les données à caractère personnel inexactes qui se rapportent à elle et faire effacer ou interdire d'utilisation les données incomplètes ou non pertinentes au regard de la finalité du traitement (68). Si des données inexactes, incomplètes ou non pertinentes ont été transmises à des tiers ou au public, le responsable doit, dans le mois qui suit l'introduction d'une requête en rectification portant sur ces données, communiquer les corrections ou effacements à effectuer aux personnes à qui ces données ont été communiquées. Le responsable est cependant libéré de cette obligation lorsqu'il n'a plus connaissance des destinataires de la communication ou lorsque la notification paraît impossible ou implique des efforts disproportionnés.

(66) Art. 13 nouveau de la loi du 8 décembre 1992.

(67) Voy. Y. Poullet et B. Havelange, *op. cit.*, pp. 233 et s. Les auteurs prônent un système d'accès direct aux données « policières » enregistrées, accompagné de la possibilité pour les organismes en cause d'opposer un refus motivé à l'accès direct, auquel cas un accès indirect par un intermédiaire tel la Commission de la protection de la vie privée peut être exercé.

(68) Art. 12, § 1er, al. 1 et 5 nouveaux de la loi du 8 décembre 1992.

D. Sanctions et recours

1. Sanctions pénales

La loi prévoit une sanction pénale à l'encontre du responsable du traitement qui n'a pas fourni aux personnes concernées les informations requises (69). Une sanction est également réservée au responsable qui n'a pas donné communication, dans les quarante-cinq jours de la réception d'une demande d'accès, des renseignements demandés, ou qui a donné sciemment des renseignements inexacts ou incomplets (70). Dans les deux cas, le responsable est passible d'une amende allant de cent à cent mille francs.

2. Recours

En cas de difficultés rencontrées dans l'exercice du droit d'accès, la personne concernée peut adresser une plainte à la Commission de la protection de la vie privée. Cette commission ne remplit pas exactement une fonction d'organe de recours administratif, mais elle peut effectuer une mission de médiation qui amènerait le responsable du traitement à respecter les obligations que lui impose la loi. En cas d'insuccès, la Commission dénonce l'infraction constatée au procureur du Roi et peut soumettre le litige au président du tribunal de première instance (71).

Une action spéciale est prévue auprès du président du tribunal de première instance, siégeant comme en référé, pour les personnes qui ont vu leur demande d'accès rejetée ou à laquelle il n'a pas été donné suite dans le délai prescrit (72).

(69) Art. 39, al. 1er, 4° nouveau de la loi du 8 décembre 1992.
(70) Art. 39, al. 1er, 5° de la loi du 8 décembre 1992.
(71) Art. 32, § 2 de la loi du 8 décembre 1992.
(72) Art. 14 de la loi du 8 décembre 1992.